



Release Notes for Device Fault Manager 1.1 on Windows 2000 and Windows NT

These release notes are for use with CiscoWorks2000 Device Fault Manager (DFM) 1.1 running on a Windows platform. Supported Windows versions are:

- Windows NT Workstation 4.0, Service Pack 6a
- Windows NT Server 4.0, Service Pack 6a
- Windows 2000 Professional and Server, Service Pack 1

These release notes provide:

- New Features
- Documentation Roadmap
- Additional Information Online
- Documentation Addenda
- Documentation Errata
- Device Fault Manager Known Problems



Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2001. Cisco Systems, Inc. All rights reserved.

78-12194-02

- Obtaining Documentation
- Obtaining Technical Assistance

New Features

Device Fault Manager 1.1 contains the following new features:

- Additional device support
- New GUI menus for managing the DFM inventory:
 - Scheduling device discovery
 - Synchronizing the Resource Manager Essentials device list with the DFM inventory
- New GUI menus for configuring DFM adapters:
 - Configuring DFM trap receiving and forwarding
 - Configuring the Mail Notifier Adapter to send mail notifications to recipients
 - Configuring the Trap Notifier Adapter to forward traps handled by DFM to specified recipients
 - Configuring the File Notifier Adapter to log DFM alarms to a file

Documentation Roadmap

The following documents are provided in PDF on your product CD:

- *Device Fault Manager User Guide*
- *Installing and Setting Up Device Fault Manager on Windows 2000 and Windows NT*



Note

Adobe Acrobat Reader 4.0 is required.

Use these publications to learn how to install and use DFM:

- *Installing and Setting Up Device Fault Manager on Windows 2000 and Windows NT* (DOC-7810607=)—Provides instructions for installing DFM on a Windows system, and offers quick-start steps for using DFM. This publication is available on the CD-ROM in PDF format. The filename is win_inst.pdf.
- *Device Fault Manager User Guide* (DOC-7810608=)—Describes DFM and provides instructions for configuring, administering, and operating it. This publication is available on the CD-ROM in PDF format. The filename is dfm_ug.pdf.
- DFM online help—Contains all of the information available in the *Device Fault Manager User Guide*. This ensures you have complete information even if you do not have the manual readily available while using DFM.

Use these publications to learn how to install and use CD One:

- Release Notes for CiscoWorks2000 CD One, 4th Edition on Windows 2000 and Windows NT (DOC-787121=)—Describes CD One, 4th Edition known problems, explains how CiscoWorks2000 handles time zone issues, and provides sources for getting additional general information.
- *Installing and Setting Up CD One on Windows 2000 and Windows NT* (DOC-787199=)—Describes installing and preparing to use CD One, and troubleshooting CD One installations.
- *Getting Started with the CiscoWorks2000 Server* (DOC-787167=)—Provides an overview of the administrative functions provided by the CiscoWorks2000 Server, which is used by DFM and all CiscoWorks2000 applications.

Additional Information Online

For information about CiscoWorks2000 Device Fault Manager supported devices, refer to the following URL, or check the documentation on Cisco.com for the correct location.

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/dfm/dev_sup/index.htm

**Note**

DFM does not support switch clusters. A switch cluster is a group of switches that comprise a master switch and slave switches. This relationship allows network management systems (NMSs) to query the master switch for information about the slave switches.

Documentation Addenda

The following information is missing from the hardcopy, online help, or PDF versions of the DFM documentation. The documentation on Cisco.com has been updated with this information.

DFM Installation and Occupied Ports

During installation, if DFM detects another application using port 162, DFM displays the following message:

```
WARNING: Installation has detected port 162 in use. DFM is set to use
port 9000 for receiving SNMP traps.
```

If you see this message during installation, refer to *Installing and Setting Up Device Fault Manager*.

DFM Device Naming Convention

A device can be discovered either from a seed file or by using Add Agent from the DFM consoles. To assign a name to the discovered device, DFM uses the following algorithm:

1. DFM obtains a value of sysName from the device SNMP agent.
2. DFM tries to resolve sysName and obtain the IP addresses from DNS:
 - a. If the DNS lookup for sysName succeeds and returns an IP address (or addresses) associated with the SNMP agent, sysName becomes *nodename*.

- b. If the DNS lookup for `sysName` fails, DFM checks to see if either the seedfile or Add Agent procedure specified the device as a name. If it did, the seedfile name becomes *nodename*.
- c. If the DNS lookup for `sysName` fails and the device was not specified as a name, DFM checks to see if either the seedfile or Add Agent procedure specified the device as an IP address. If it did, DFM tries to resolve the IP address from DNS:
 - If the DNS lookup for the IP address succeeds and returns a name, this name becomes *nodename*.
 - If the DNS lookup for the IP address fails, the seedfile IP address becomes *nodename*.

This approach emphasizes the importance of specifying DNS resolvable names as `sysName`; otherwise the IP address may be used.

Both Windows NT and Windows 2000 can be configured to use NetBios over TCP/IP. If NetBios over TCP/IP is used and a DNS lookup fails, the Windows NT and Windows 2000 name resolver continues searching using NetBios name resolution. As a result, certain hosts (either Windows-based hosts or Windows-based router cards, such as the Cisco CallManager) might be named according to their NetBios names. Because these names might not immediately correspond to any IP address or DNS name, this could confuse users. Additionally, in certain cases the NetBios name resolution might depend on device status—for example, if a device is up and responding to NetBios name queries, its name will be resolved.

To avoid confusion, disable NetBios over TCP/IP on any Windows NT or Windows 2000 servers running DFM. If this solution is unacceptable, make sure NetBios names are consistent with the DNS naming scheme.

Conditions for Changing the Default Polling Threshold

The polling threshold is set to four minutes, by default. You may want to adjust this threshold depending on your network configuration—specifically:

- Geographic area your network covers.
- Number of routers, switches, and other objects managed by DFM.
- Number of trunk ports managed by DFM.
- DFM server configuration, such as memory or processor speed.

A useful method for changing this threshold is to create a group and then assign a threshold to that group. For example, you might want to create a group of four or five routers and set those routers to poll every 30 seconds. For more information on groups and settings, refer to the *Device Fault Manager User Guide* (available from online help).

Creating New Groups

Keep these points in mind when creating a group:

- Because groups created without any settings are not polled, be sure to map settings to any groups you create.
- If you do create a group without any settings, do not manage any ports in the group. Although managing such ports is allowed, no MIBs will be polled.
- Regardless of the settings you attach to a group, default polling is done where the default MIBs are queried.

For more information on groups and settings, refer to the *Device Fault Manager User Guide* (available from online help).

Subscribing to Multiple Events with a Notification Adapter

The *Device Fault Manager User Guide* describes how to configure adapters to subscribe to particular events. To configure a single notification adapter to subscribe to diverse classes and events, add the following code fragments to the appropriate notification adapter configuration file:

```
SubscribesTo =
{
    GA_ChoiceSubscription::Name-All-Subscriptions
    {
        # Subscribe to events whose class, instance, and event
        # names match the given pattern.
        className = "class"
        instanceName = ".*"
        eventName = "event"
        aggregates = {TRUE|FALSE}
        symptoms = {TRUE|FALSE}
    },
    GA_ChoiceSubscription::Name-All-Subscriptions
    {
        # Subscribe to events whose class, instance, and event
        # names match the given pattern.
        className = "class"
        instanceName = ".*"
        eventName = "event"
        aggregates = {TRUE|FALSE}
        symptoms = {TRUE|FALSE}
    }
}
```

Keep the following in mind:

- *Name* must be unique.
- Separate each GA_ChoiceSubscription code fragment with a comma (except for the last fragment).
- Provide values for *class* and *event* according to the list on pages 10-9 through 10-12 of the *Device Fault Manager User Guide*.
- Specify TRUE or FALSE depending on whether or not you want to subscribe to aggregates (compound events) and symptoms.

For example, to configure the Mail Notifier Adapter to track all router and switch aggregates (compound events), along with all chassis symptoms, add the following to the Mail Notifier Adapter configuration file:

```
SubscribesTo =
{
    GA_ChoiceSubscription::Router-All-Subscriptions
    {
        # Subscribe to events whose class, instance, and event
        # names match the given pattern.
        className = "Router"
        instanceName = ".*"
        eventName = ".*"
        aggregates = TRUE
        symptoms = TRUE
    },
    GA_ChoiceSubscription::Switch-All-Subscriptions
    {
        # Subscribe to events whose class, instance, and event
        # names match the given pattern.
        className = "Switch"
        instanceName = ".*"
        eventName = ".*"
        aggregates = TRUE
        symptoms = TRUE
    },
    GA_ChoiceSubscription::Chassis-All-Subscriptions
    {
        # Subscribe to events whose class, instance, and event
        # names match the given pattern.
        className = ".*"
        instanceName = ".*"
        eventName = ".*"
        aggregates = FALSE
        symptoms = TRUE
    }
}
```

Documentation Errata

The following documentation errata is in the hardcopy, product online help, or PDF versions of the DFM documentation. The documentation on Cisco.com has been updated with these corrections.

**Note**

In the following topics, *NMSROOT* represents the CiscoWorks2000 installation directory (by default, C:\Program Files\CSCOPx).

Exporting DFM 1.0 Information to an Upgraded Remote Host

On page 2-14 of *Installing and Setting Up Device Fault Manager on Windows 2000 and Windows NT*, in the section “Exporting DFM 1.0 Information to an Upgraded Remote Host,” step 10 instructs you to issue these commands:

```
C:\> cd NMSROOT\rigel\scripts
C:\> NMSROOT\bin perl import_dfm.pl
```

When you add the path *NMSROOT\bin* before the perl command, the machine cannot resolve the path and does not execute the script.

The workaround is to issue the perl command without specifying the path *NMSROOT\bin*, as follows:

```
C:\> cd NMSROOT\rigel\scripts
C:\> perl import_dfm.pl
```

Unregistering and Reregistering Adapter Daemons

The following pages in *Installing and Setting Up Device Fault Manager on Windows 2000 and Windows NT* are missing instructions for unregistering and reregistering adapter daemons:

- Pages 2-4 and 2-5, Step 12
- Pages 2-10 and 2-11, Step 13
- Pages 2-17 and 2-18, Step 14

A process cannot be unregistered if any running processes depend on it. This is the sequence for unregistering the DFM processes:

1. Unregister the notification adapter processes (which depend on the DfmServer process).
2. Unregister the DfmServer process (which depends on the DfmBroker process).
3. Unregister the DfmBroker process.

To reregister the processes, perform these steps in reverse.

Step a and Step c should therefore read as follows:

- a. Unregister the daemons with the daemon manager:

- For DFM notification adapters:

```
# NMSROOT\bin\pdcmd.exe -u DfmFileNotifier
# NMSROOT\bin\pdcmd.exe -u DfmTrapNotifier
# NMSROOT\bin\pdcmd.exe -u DfmMailNotifier
```

- For DfmServer:

```
# NMSROOT\bin\pdcmd.exe -u DfmServer
```

- For DfmBroker:

```
# NMSROOT\bin\pdcmd.exe -u DfmBroker
```

- b. (Refer to *Installing and Setting Up Device Fault Manager on Windows 2000 and Windows NT*; this step is correct as is.)

- c. Re-register the daemons with the daemon manager, specifying the clients that can connect to the broker and server (in this example, the DFM broker port is 9002 and lucy and ethel are the clients):

- For DfmBroker (the following command is one line):

```
# NMSROOT\bin\pdcmd.exe -r DfmBroker -e NMSROOT\objects\smarts\bin\brstart.exe -f
"--output --port=9002 --accept=lucy,ethel
--restore=NMSROOT\objects\smarts\conf\broker.rps"
```

- For DfmServer (the following command is one line):

```
# NMSROOT\bin\pdcmd.exe -r DfmServer -e NMSROOT\objects\smarts\bin\sm_server.exe -d
DfmBroker -f "--bootstrap=DFM_bootstrap.conf --accept=lucy,ethel --output --name=DFM"
```

- For DFM notification adapters (the following commands are each one line, and will register the adapter processes to automatically start upon reboot):

```
# NMSROOT\bin\pdcmd.exe -r DfmFileNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=filelog --output=sm_file_notifier"
```

```
# NMSROOT\bin\pdcmd.exe -r DfmTrapNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=trap --output=sm_trap_notifier"
```

```
# NMSROOT\bin\pdcmd.exe -r DfmMailNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=mail --output=sm_mail_notifier"
```

If you do not want the daemons to start after a reboot, add the `-n` option to the end of the command, as in this File Notifier Adapter example:

```
# NMSROOT\bin\pdcmd.exe -r DfmFileNotifier -d DfmServer -e
NMSROOT\objects\smarts\bin\sm_notify.exe -f "--adapter=filelog --output=sm_file_notifier"
-n
```

DFM Process Dependencies

Page 11-11 of the *Device Fault Manager User Guide* lists the `DfmChangeProbe` process as being dependent on the `EssentialsDbEngine` and `DfmServer` processes. This is not correct. The `DfmChangeProbe` process depends on the `EssentialsDbEngine` and `EssentialsDbMonitor` processes.

Using the Command Line

In the *Device Fault Manager User Guide*, most command line interface (CLI) commands represent the UNIX command convention. For example, the following command is from page 6-13, and extracts a list of SNMP agents for a seed file:

```
# NMSROOT/objects/smarts/bin/sm_tpmgr -s DFM --dump-agents > seedfile.txt
```

For Windows platforms, the proper syntax would be:

```
# NMSROOT\objects\smarts\bin\sm_tpmgr.exe -s DFM --dump-agents > seedfile.txt
```

Unless otherwise noted, all Windows CLI commands should have an .exe suffix. For example, to find out how many trunk and access ports are currently imported into DFM (from page 1-7 of the hardcopy and PDF versions of the installation guide), use this command:

```
# NMSROOT\objects\smarts\bin\sm_tpmgr.exe --server=DFM --sizes
```

Device Fault Manager Known Problems

Known problems are unexpected behaviors or defects in DFM software releases. They are graded according to severity level. These release notes contain information for severity levels 1 and 2, and information on significant severity level 3 known problems.

You can search for known problems on the Cisco bug tracking system tool, called Bug Navigator II.

To access Bug Navigator II, enter <http://www.cisco.com/support/bugtools> in your web browser or log into Cisco.com and select **Service & Support > Technical Assistance Center > Tools > Software Bug Toolkit > Bug Navigator II**.

Table 1 *Device Fault Manager Known Problems*

Bug ID	Summary	Explanation
CSCdt22462	6 minute delay while downloading console on Win2K	Refer to the Release Notes for CiscoWorks2000 CD One, 4th Edition, for more information.
CSCdt27758	Notification process not seen in CW2K desktop process status	<p>When a user disables any of the notification adapter processes, the processes are unregistered from CiscoWorks2000 and are not displayed when the user selects Server Configuration > Administration > Process Management. Conversely, when a user enables the processes, the processes are registered and are displayed.</p> <p>There is no workaround. This action occurs by design and is documented in the DFM user and installation guides.</p>
CSCdr21203	Install on Windows does not always reboot, causing server to fail	<p>At the end of a DFM installation on Windows 2000 and Windows NT, the installation program asks the user to select reboot to reboot the machine. However, occasionally Windows 2000 and Windows NT are only restarted, and the machine is not rebooted. Because the installation adds registry entries, DFM will not operate correctly if the machine is not rebooted. This is a known bug in InstallShield 5.5.</p> <p>The workaround is to manually reboot the machine.</p>
CSCdt57822	Cat3548XL memory/processor support?	<p>Certain IOS-based devices (such as the 3548XL) are not fully supported in DFM 1.1. These devices will be fully supported in an upcoming Incremental Device Support (IDS) package.</p> <p>There is no workaround.</p>

Table 1 Device Fault Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdr31406	HELP option needs to be replaced with VERSION	The Help menu located on the DFM consoles contains DFM software version information, not online help about the DFM product. To access the DFM online help, use the CiscoWorks2000 Help button located above the CiscoWorks2000 navigation tree.
CSCdt15420	Adding MSFC/RSFC/RSM IP address individually doesn't classify	<p>When an MSFC/RSFC/RSM IP address is added to DFM, but the parent switch IP address has not yet been added, the MSFC/RSFC/RSM is discovered but added only in the IP class.</p> <p>The workaround is to add the parent switch first.</p> <p>Note If the MSFC/RSFC/RSM SNMP community string is different from that of the parent switch, DFM will not discover the MSFC/RSFC/RSM. You must explicitly give the MSFC/RSFC/RSM IP address and community string. DFM will then discover them after discovering the parent switch.</p>

Table 1 Device Fault Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt15538	Inconsistent Monitoring Consoles	<p>Monitoring Consoles have a different display, depending on where you launch them from:</p> <ul style="list-style-type: none"> • If you use the Administration Console toolbar button, the Monitoring Console displays the Inventory Browser. • If you select File>New>Monitoring Console from any running console, the Monitoring Console displays the Inventory Browser. • If you use Device Fault Manager>Monitoring Console, the Monitoring Console does not display the Inventory Browser. <p>The workaround is to manually change the layout of your consoles as described in the <i>Device Fault Manager User Guide</i> (available from online help).</p>
CSCdt61184	Managed - Unmanage menus are not working in Administration Console	<p>After a user unmanages an element using the Administration Console Edit>Unmanage option, the Edit>Manage option becomes disabled.</p> <p>The workaround is to right-click the element and select Manage, or go to another device and click Back.</p>
CSCds27261	Monitoring Console allows the user to make changes to attributes	<p>When a user logs into the CiscoWorks2000 console as administrator and invokes the Administration or Monitoring Console, the user can change Monitoring Console attributes. (Users logging in without administrator privileges cannot change these attributes.) If the administrator logs out without exiting the browser, users with lesser privileges can log in and change the attributes.</p> <p>The workaround for making sure users without administrator privileges cannot change the attributes is to log out and exit the browser.</p>

Table 1 Device Fault Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCds84738	FXS voice port returns value as Other when Dormant	Currently the router interfaces monitored by DFM show status Up, Down, or Other. Because Dormant or any other status mentioned in the description is not recognized, any status other than Up or Down is displayed as Other. Products running on DFM import status information for Routers from DFM; hence dependent products will also show the status as Other.
CSCdt61923	Right-clicking events at bottom of Monitoring Console throws NullPoint	<p>On Windows 2000, if a user selects an alarm from a Monitoring Console and right-clicks it, but the Monitoring Console is at the bottom of the window, the drag-and-drop menu throws a NullPointerExpection.</p> <p>The workaround is to select the alarm and then use the Monitoring Console Event menu instead of right-clicking the alarm.</p>
CSCdr91450	Long discovery period causes time out	<p>When DFM discovers Catalyst 3524XL devices, and the devices are running 12.0(5.1)XP, SNMP requests may time out.</p> <p>The workaround is to upgrade Catalyst 3524XL devices to 12.0(5)XU or later.</p>
CSCdr93198	GUI: Trend View shows the Future data in graph	<p>Periodically, the DFM TrendView shows future data in the graph.</p> <p>There is no workaround. TrendView is not supported in DFM 1.0 or 1.1.</p>
CSCdr97458	Invoking a script from Monitoring console doesn't work	<p>In the Monitoring Console, if a user selects Event>Script and supplies a script, nothing happens.</p> <p>There is no workaround. This functionality is not supported in DFM 1.0 or 1.1.</p>

Table 1 Device Fault Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdr98754	Certainty value is always 100%	<p>In the Alarm log, by design, all events have a Certainty value of 100%. DFM analysis does not include partial relationships—for example, 4 of 4 symptoms means 100% certainty that the problem is known; 3 of 4 symptoms means 75% certainty; and so forth. DFM 1.0 displays alarms only when all correlation criteria have been met, so the certainty for displayed alarms is always 100%.</p> <p>There is no workaround.</p>
CSCds26001	Installing DFM in machine without OV/NV gives warning	<p>When installing DFM, if HP OpenView or NetView are not detected during the DFM installation process, the installation program displays this message:</p> <p>WARNING: Neither HP-OpenView or NetView installed.</p> <p>However, this message is misleading, because DFM does not require HP OpenView or NetView.</p> <p>There is no workaround. Ignore the message.</p>
CSCdt69972	Import_dfm.pl should ask user to initiate rediscovery	<p>After a user issues the import_dfm.pl command to import DFM data from a remote host, the device information in the DFM repository may be out of date. The user should initiate a rediscovery of all devices to make sure that DFM reflects the current state of managed devices.</p> <p>To rediscover all devices, select Inventory > Inventory Collect All from the Administration Console.</p>
CSCdt91653	Clicking on open console should bring window to foreground	<p>When a user clicks on an open Administration or Monitoring Console, DFM should bring the console window to the foreground (instead of displaying a message that the console is already running).</p> <p>There is no workaround.</p>

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online

technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “Documentation Roadmap” section.

AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, CiscoLink, the Cisco NetWorks logo, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0102R)

Your right to copy the software and this documentation is limited by copyright law. Making unauthorized copies, adaptations, or compilation works is prohibited and constitutes a punishable violation of the law. Use of the software is governed by the license agreement accompanying such software.

The documentation is provided “as is” without warranty of any kind. In no event shall System Management ARTS Incorporated be liable for any loss of profits, loss of business, loss of use of data, interruption of business, or for indirect, special, incidental, or consequential damages of any kind, arising from any error in this documentation.

InCharge, the InCharge logo, SMARTS, the SMARTS logo, “Minds Over Networks,” and “Ensuring Peak Availability and Performance of E-Business” are trademarks or registered trademarks of System Management ARTS Incorporated.

SMARTS uses the FLEXIm licensing product. FLEXIm is a trademark of Globetrotter Software Inc. For product information, search the web site, www.globetrotter.com.

All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright 1996-2001 by System Management ARTS Incorporated. All rights reserved.

InCharge makes use of ptmalloc, a multi-threaded malloc implementation that includes the following notice.

Copyright (c) 1997 Wolfram Gloger.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the name of Wolfram Gloger may not be used in any advertising or publicity relating to the software.

THE SOFTWARE IS PROVIDED “AS-IS” AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL WOLFRAM GLOGER BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright © 2001, Cisco Systems, Inc.
All rights reserved.